THE DoD OF TOMORROW:

Innovating American Defense

cont

ents

executive summary

In 2015,

*we still **talk about wars** that started in the early 2000s, **manage tense state relations** first established during the Cold War, and **leverage weapon systems** built to combat the Axis powers.*

But don't be fooled. The mission and tactics of the Department of Defense are changing — and fast.

In his **first letter** to DoD personnel, Secretary Ash Carter impressed the need for transformation in stating, "We must be open to change in order to operate effectively in an increasingly dynamic world; to keep pace with advances in technology; and to attract new generations of talented and dedicated Americans to our calling."

Yet for the United States' oldest and largest government agency, change is no easy task. More than 3 million personnel span every time zone and leverage a wide variety of technologies and tactics to achieve a fluid mission.

So what will it take to transform DoD?

Any modifications to strategy or operations will have to be comprehensive and scalable. In this guide, we examine how:

- Improved operations will create a more agile, data-driven defense strategy
- New technologies will offer strategic advantage in every battle space
- Enhanced workforce tactics will recruit and train the next-generation warfighter
- Revamped acquisition programs will ensure ongoing transformation

In order to accomplish real change, DoD will dedicate significant resources to overhauling every component of its organization. This guide offers examples of current initiatives and explores how the Pentagon will transform American defense.

The Changing Mission of DoD

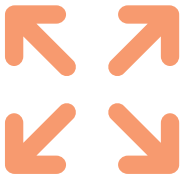
In this guide, we examine a broad range of initiatives that DoD is deploying to transform itself and its operations. But before we dive into how the department is changing, we should explore why it's changing. Evolving threats, battle lines, and responsibilities are three large challenges forcing Pentagon officials to rethink their tactics.

NEW THREATS

In front of the House Armed Services Committee's Emerging Threats and Capabilities Subcommittee, Army General Joseph L. Votel **called 2014** the most "complex" year for DoD in the past half century. Unfortunately, that was indeed a fair statement.

In addition to encountering the same state actors that challenged U.S. interests during the Cold War, the Pentagon also has new states to secure or confront. At the same time, there is an abundance of non-state actors who challenge security, and they are better connected, even "hyper-connected," via the Internet and enhanced telecommunications.

Even disregarding malicious actors, the threats of the 21st century seem innumerable. A recent **Defense Advanced Research Projects Agency (DARPA) report** calls out global economic inequality, demographic shifts, urbanization, human and animal pandemics, social unrest, energy crises, and environment degradation as just a few of the challenges DoD must tackle if true security is to be achieved.



BIGGER BATTLESPACE

These threats are also more pervasive in their reach. When you recall wars of the 20th century, you probably think of places like the Western Front or the Pacific Theater because battles were principally fought on land, in the air, or at sea.

Compare that to today's military operations and you'll notice a stark contrast. The strategic environment is global and DoD must fight what Deputy Secretary Robert Work **calls** "hybrid wars" that transcend the traditional battle space.

To fight these hybrid wars, **Joint Vision 2020**, a report by the Joint Chiefs of Staff examining threats and possible responses arising between 2010 and 2020, set the goal of accomplishing "full spectrum dominance." That means that the military force of today must not only be able to control the traditional domains of air, land, and sea; it must also be able to win wars in outer space and, even more challenging, cyberspace.

MORE ROLES

Within each of these domains, the responsibilities of DoD are also evolving. While its official moniker isn't changing, the Department of Defense, Security, and Stability may be a more appropriate label for the agency.

Consider the roles that U.S. warfighters played in the recent wars in Iraq and Afghanistan. Not only did they have to execute traditional defensive maneuvers to defeat the enemy but, once each battle space was infiltrated, DoD personnel also had to secure networks against hackers, win the hearts and minds of locals, train new militaries, and rebuild damaged infrastructures.

Even as troops withdraw from both theaters, these roles of security and stability will continue to be required of American forces worldwide. If anything, these responsibilities will only expand as new threats continue to mount. Last year, former Defense Secretary Chuck Hagel **even challenged DoD** to plan for securing the nation in the face of climate change, for instance.

With so many challenges laid at DoD's feet, it wouldn't be surprising to find the agency overwhelmed and static. This is especially tempting if you consider the shrinking budget, workforce gaps, and resource constraints that also hinder operations.

Nevertheless, agency officials are determined to find a way forward. In fact, DoD is already taking the initiative to change its operations, technology, workforce, and acquisitions strategies to meet its 21st-century challenges. The next sections in this guide explain how defense leaders will execute this organization-wide transformation.


opera

DoD is known for

silos, bureaucracy, set practices, and a command-and-control mentality. However, to confront new threats with new tactics in the moment, officials will have to reconsider the way it operates. Agility, collaboration, consolidation, and informed decision-making will drive the Pentagon forward.

ations

CONSOLIDATING & STANDARDIZING OPERATIONS

Because we reference it as a single department, it's easy to think of DoD as one integrated organization that synchronously strategizes and executes on defense imperatives. Yet if you consider the various military branches, internal agencies, and personnel scattered globally, you will quickly realize that DoD is really an amalgam of many moving parts and tactics. Nevertheless, coordination is required, especially as DoD's mission expands.

One way the Pentagon hopes to achieve that coordination is to standardize operations and break down organizational silos. To that end, the **Defense Standardization Program** was established in 2011 to "identify, influence, develop, manage and give access to standardization progress, products, and services." It does so by producing projects in-house and **awarding other personnel teams** for their innovative standardization achievements.

Outside the formal program, other defense agencies are also getting in the game. The relatively new **Defense Health Agency** is **embracing standardization**, with a particular focus on streamlining data collection and employee health records. DoD's **recently announced** digital service will aid in this endeavor. Additionally, the Office of the Deputy Chief Management Officer is **standardizing business functions** such as accounting, personnel management, and human resources to produce clean financial audits by 2017 — a goal the 2010 National Defense Authorization Act established.

Perhaps the most striking exemplar of this move toward consolidation and standardization is the framework for a **Joint Information Environment** (JIE), an ambitious multi-year plan to converge all of DoD's communications, computing, and enterprise services into single information and security architecture. It will consolidate data and operations centers, and also promulgate standards for the information shared across locations and forces.

As part of JIE, DoD CIO Terry Halverson **announced** plans to replace all local security architectures with joint regional security stacks (JRSS), "a single set of servers, tools, and software that will provide better command and control and more security...at a lower cost," by 2017. **Joint Base San Antonio** was the first to complete its transition to JRSS just last year. However, Halverson also explained that there would always be more to do, because JIE is a concept that will continue to evolve.

"Identify, influence, develop, manage and give access to standardization progress, products, and services."

GOAL OF THE DEFENSE STANDARDIZATION PROGRAM

ENABLING AGILE PROJECT MANAGEMENT

To support that constant evolution of JIE and other projects, DoD's project management strategies must become more adaptive. Some defense leaders have already realized this and included a mandate for that dexterity in the **2010 Defense Authorization Act**.

The act states, "The Secretary of Defense shall develop and implement a new acquisition process for information technology systems… designed to include:

- Early and continual involvement of the user;
- Multiple, rapidly executed increments or releases of capability;
- Early, successive prototyping to support an evolutionary approach; and
- A modular, open-systems approach."

In other words, DoD officials decided to embrace Agile (with a capital A). This project management process contrasts traditional, comprehensive planning techniques, such as the Waterfall or Spiral methods, which lock down a design in advance of development and then bank on capabilities being realized in the final stages of project execution.

Agile works differently by developing a minimum viable product through asynchronous, cross-disciplinary collaboration and then releasing it for testing, knowing that those tests will likely expose faults in the design. It's an iterative approach to both procurement and development, designed to cut costs while deploying better tech in shorter amounts of time.

At the time, it was an especially surprising turn for DoD, considering that many other agencies weren't taking on the development process. But the need to cut large defense budgets, keep projects running on time, and equip soldiers with up-to-date technology was imperative to change.

Scrum Inc., a private company that champions the use of Agile in the defense sector, offered a recent comparison to prove the value of this new approach. Company officials **cited** the F-35, a fighter jet project that was $143 billion over budget and significantly delayed, as a key example of how the Waterfall system fails the defense industry. When the **Government Accountability Office investigated** the F-35 delay, researchers concluded that project challenges were "due largely to delays in software delivery, limited capability in the software when delivered, and the need to fix problems and retest multiple software versions."

The company compared the F-35 project to a similar Swedish stealth fighter, Saab JAS 39E Gripen, which was built using Agile methods. The fighter was produced on schedule, and cost only $43 million. Its software, a key differentiator for any modern fighter jet, is updated every six months and it's **increasingly growing in popularity** with each cycle.

DoD officials hope to realize the same benefits of reduced costs and timely deployment by using Agile at home. To some extent, they are making progress in adoption.

For instance, the Defense Information Systems Agency (DISA) launched the first iteration of its **Defense Department Mobility Unclassified Capability** (DMUC) last year. The program, intended to allow more than 100,000 users access to DoD's Information Network (DoDIN) through a wide variety of mobile platforms and devices, was initially released with minimal applications and only on iOS devices. However, the launch began a "90-day spiral approach" by which the software will be updated with new features and applications every quarter.

"The mobility program is not business as usual for IT procurements," DISA said in a **press release**. "DISA is working to create a secure adaptive mobile environment necessary to incorporate the steady advancement of technology, including application development, changing security architecture requirements, and continuous enhancement of equipment."

DMUC is already advancing in its complexity and efficacy, so why isn't the program "business as usual"? After all, agility of operations was first mandated in 2010.

Many, including **Stephen Welby**, Deputy Assistant Secretary of Defense for Systems Engineering, say the biggest challenges to Agile implementation across DoD are misperceptions, rather than concrete barriers. Beliefs that Agile projects take on more risk, disallow oversight, or don't fit with available contracting vehicles hinder adoption even as experts assert their invalidity.

POWERING DECISIONS WITH DATA

So how will DoD dispel these misperceptions? One convincing way is to make the case with data, as Scrum did when it compared the results of the F-35 and JAS 39E Gripen projects. However, to really inform DoD operations with data may be more challenging.

DARPA **calls the increase** in available data an "information explosion," which seems apt when you consider that the agency anticipates $5x10^{21}$ bytes of data to be generated by 2020. This abundance of information is both a blessing and curse for DoD.

On one hand, this data can tax existing IT systems and overwhelm analysts trying to find significance in the noise. However, when performed correctly, "Big data analytics are offering glimpses of a possible future in which sophisticated models will be able to recognize the first inklings of epidemics, ailing ecosystems, and even potentially dangerous geopolitical threats, allowing time to mitigate looming impacts," states a **2015 report**.

With this much potential, DoD can't ignore big data. Therefore, the Pentagon is seeking strategies and technologies that can transform unordered data from unmanned aerial vehicles, satellite imaging systems, troops on the ground, and other weapons systems into insights.

DARPA is leading the charge, committing more than **$164 million in fiscal 2016** to programs such as **XDATA**, an open source software library for big data tools and techniques; and **Big Mechanism**, a program developing technology to read research materials and intelligently extract causal relationships; and **GRAPHS**, which seeks to discover scalable algorithms to handle DoD-wide data for operational gains.

However, it isn't the only department looking to turn data into decisions. DISA developed an analytical cloud, **Acropolis**, to gather, store, and analyze data from across DoD. Collected information is used to analyze DoDIN, inform the Continuous Monitoring and Risk Scoring program, and ultimately guide DoD's cyber tactics. And the Air Force is taking a different approach, allowing the public to help sort through massive amounts of data on the **Collaboratory** website.

"Big data analytics are offering glimpses of a possible future in which sophisticated models will be able to recognize...potentially dangerous geopolitical threats, allowing time to mitigate looming impacts."

DARPA 2015 REPORT:
"BREAKTHROUGH TECHNOLOGIES FOR NATIONAL SECURITY"

RESOURCES

ENABLING THE JOINT INFORMATION ENVIRONMENT

DISA, 2014

Brief defining the strategic vision and implementation plan for JIE

THE JOINT INFORMATION ENVIRONMENT: THE IT FRAMEWORK OF THE FUTURE

GovLoop, 2014

Research guide explaining the mission, details, and progress of JIE

CHANGE CULTURE, NOT JUST TECHNOLOGY

GovLoop, 2015

Infographic examining how to incorporate Agile project development into institutional culture

THINKING ABOUT AGILE IN DOD

Stephen Welby, Deputy Assistant Secretary of Defense for Systems Engineering, 2013

Presentation detailing Agile development processes, challenges, and solutions in defense settings

TANIUM™

With Tanium you can answer critical questions about the current state of your endpoints & take immediate action as needed. Across all of your systems globally.
All within 15 seconds.

ASK
your question in plain English

KNOW IN 15 SECONDS
what is happening across all of your endpoints

- How many laptops are missing critical security patches?
- How many unmanaged machines are on my network?
- What versions of Java are out of date in my environment?

ACT
change all impacted endpoints as needed

15-Second Visibility & Control Over Every Endpoint. Even Across the Largest Networks.

Impossible? Think again.

Let us show you the magic of Tanium.

Learn more at www.tanium.com

Maintaining Endpoint Security Across an Expansive Network

An interview with Ralph Kahn, Vice President Federal at Tanium

The Department of Defense's information network spans the globe. Yet while that asset is necessary to support a distributed workforce and worldwide mission, it also widens the potential attack surface for cyberthreats. At the same time, the sophistication and rate of cyberattacks are rapidly increasing.

This heightened vulnerability cannot be ignored. To understand how DoD can reduce its risk exposure, we spoke with Ralph Kahn of Tanium, an endpoint security platform provider.

"It's incumbent on every agency to protect the data they collect and the systems that process it, from a very large and growing array of cyberthreats," Kahn said. He also explained how rapid, scalable endpoint monitoring will allow DoD to reap the benefits of its expansive IT network, without sacrificing the security of its data.

ACCELERATING DETECTION

Kahn said the most critical barrier to security is the inability to monitor your endpoints in real time. "The bad guys are moving really fast and DoD agencies, with their existing processes, procedures, and technologies, have a really hard time keeping up," he said. "Most of the endpoint technologies that DoD agencies are operating with, and most of the processes and procedures that they've developed to operate them, are based on a cycle time that's measured in days or weeks, not a cycle time that's measured in seconds."

According to Kahn, cycle times measured in days or weeks leave a large time window in which adversaries can operate. "The adversary operates in seconds," he said. "They penetrate your system, they figure out what they can do and move around, all in a matter of seconds."

In many cases, agencies do have the ability to spot these intrusions using existing network security technology. Yet, once an attack has been spotted, most agencies lack the ability to quickly identify how and where a threat spreads and simultaneously take action to remediate it.

Tanium's security platform is unique in its ability to provide real time detection and remediation of threats. Tanium can query every endpoint in an unprecedented amount of time – less than 15 seconds in the majority of use cases. What's more, Tanium's unique architecture can provide the same response time even for organizations with hundreds of thousands or millions of endpoints.

"Tanium pairs lightning fast access to endpoint information with real time remediation capabilities," said Kahn. For DoD, this capability is crucial to ensuring that its network and endpoints remain secure even as it faces increased frequency and sophistication of cyber attacks.

Moreover, "Tanium delivers this capability in a very lightweight and powerful architecture. It does all of this on a couple of servers," explained Kahn. "That's significant because it allows you to deploy the system a lot more quickly, the lifecycle cost is a lot lower, and the availability's a lot higher."

ENSURING COMPLIANCE

In addition to providing early detection of security risks, this rapid scanning also provides visibility and regulatory benefits for DoD.

"Command Cyber Readiness Inspection, or CCRI, is a process designed to ensure that all bases across DoD have a baseline level of cybersecurity compliance, meaning patches are applied, and firewalls and other pieces of defensive hardware are properly configured," explained Kahn.

"But that process of checking to see whether they're in compliance is painful, time consuming, and expensive," he said. "The processes and technology that DoD currently use to get themselves into compliance take weeks to operate and require a large staff of people to complete them. The whole process is really disruptive to their mission."

Again, Tanium's ability to rapidly query all endpoints can eliminate risk. "Tanium can shorten that process from weeks to a day, and it can ensure very quickly that DoD bases pass their CCRIs," said Kahn. "That's a big deal because then all those people can go back to executing their missions, rather than worrying about finding vulnerabilities or keeping their computer systems up to date."

ENHANCING RESPONSE CAPABILITIES

Agencies today are awash in threat data. With recent enhancements to information sharing, agencies receive unprecedented amounts of threat data from both internal and external sources.

"The challenge for DoD is it doesn't have a method to take all that threat data and determine quickly which threats are impacting their endpoints right now," said Kahn. "Tanium's technology can take that threat data and turn it into queries which can be run across the entire department in 15 seconds. This would allow DoD to see in real time which threats were active and take immediate action to remediate them thereby reducing the threat window to minutes instead of days or weeks."

The Power of Data at DoD

An interview with Mark Krzysko, Deputy Director for Enterprise Information in the Office of the Under Secretary of Defense for Acquisition, Technology & Logistics

With over 2 million personnel, $500 million in funding, and countless tools and technologies, the Department of Defense is an organization of numbers. And each day, those assets are producing even more data as the DoD mission is executed worldwide.

To understand how the department leverages that data to better achieve its objectives, we spoke with Mark Krzysko, Deputy Director for Enterprise Information. Krzysko's objective is to facilitate innovative uses of information technologies, and the data they produce, to improve and streamline the acquisition process at DoD. He explained how and why his office is fueling the DoD Acquisition community's use of data as a strategic asset.

ENRICHING THE ROLE OF DATA

First, Krzysko offered a perspective on the evolution of data at DoD. "When we talk about integrating data [into decisions], it's not to say that we haven't used data in the past," he explained. "We've always used data to support decision-making."

However, in the past data was seen more as a requirement than a tool. "In the past, we would just look at very limited sets and we would say, 'Well, this is what we were required to collect,'" Kryzsko explained. "Now we're opening up our aperture and saying, 'Here's the problem you're trying to solve and here are potential data sets that may help you think through that problem.'"

In addition to recognizing data's potential, Krzysko said there were two changes at DoD that fostered a greater focus on data. The first was operational. "[Now], through technology, new management practices and new technologies, we're better able to access authoritative information and present it to the Under Secretary in his decision-making process," he said.

Second, scarcer resources required the department to seek ways to make better decisions. "Sequestration, the Budget Control Act, and a significant downward pressure on the department have really forced us to collaborate," Krzysko said. That collaboration has allowed organizations across DoD to more easily share data, and learn best practices for using that data to fuel better decisions.

MATCHING DATA TO PROBLEMS

Today, data is a critical tool for DoD operations. "My boss has a sign outside of his door that says, 'In God we trust. All others bring data,'" said Krzysko. "I really view data as the fuel of decision-making."

Nevertheless, Krzysko was clear that they don't simply throw massive data sets at any problem. "I always ask the first question of, 'What are you trying to achieve?'" he said.

Once a question is clarified, Krzysko and his team will provide appropriate data to inform

that query. That process involves a department-wide understanding of data sets, which is provided through an in-house framework that categorizes and defines DoD data.

"With the Acquisition Data Management Framework, we document the authoritative definition, the authoritative meaning, and the authoritative owner of that information," Krzysko explained. "We also document the general base use cases for that information. So we know, for probably the first time in many regards, who owns that piece of data, what the definition is, who owns that definition and, and what context that information will be provided to us."

Not only does this framework allow Krzysko's office to understand the nuances of particular data sets, it also gives them clear guidelines and definitions for communicating data requirements to others, including internal DoD cohorts and industry partners.

COMMUNICATING THE VALUE OF DATA

According to Krzysko, communication is a key component of their data strategy. "We have a fundamental belief that we're a communication organization that uses data, not a data organization that communicates," he said.

"We have a strong internal communication mechanism for use across the organization," Krzysko continued. "We reach out to people on the phone and meet with them constantly. We've also utilized the enterprise shared services—using their portal for our communications on. And then finally, we make sure that we have an awful lot of training. Internally, we have videos up for people to learn how to use the tools."

This communication and training is focused on empowering users to leverage data, so that they can understand its value and appropriate use. "We constantly message that we don't give you an answer; we give you an opportunity to find your answer," said Krzysko. "All we're doing is positioning the data, being transparent on what we did, how we did it, and letting the senior analyst and the business analyst do their jobs better and more efficiently. We let the decisions bear out how they would be borne out."

Beyond this messaging, Krzysko said that real-world examples also help personnel understand the value of data. "For instance, we're always going through reviews for the major weapon system programs today," he said. "Over the past month or two, we were able to fuse together obligations data capabilities with expenditure data, relative to the major programs of the Department of Defense."

Through this data synthesis, Acquisition personnel were able to shorten the time to a decision. "We're helping them through the process," said Krzysko. "And they're saying, "Oh wow, this is really good; this helps me.'"

SUPPORTING THE LARGER DOD MISSION

Krzysko was clear that the mission of his office is not to provide data for the sake of data. Instead, it's to support the broader DoD mission. "Data in and of itself is not an answer," he said. "The answer to the question lies in the value. What's my top priority? It's how we can better bring value, not only to the institution of the Department of Defense, but to the nation as a whole."

"There's not a day that I do not wake up and think about the soldier, sailor, and airmen who are out there," concluded Krzysko. "On a daily basis, we need to protect our sons and daughters. We need to protect our nation, whether it's home or abroad. That's the grand scheme here and, in my world, that all emanates from a data perspective. How can we provide data, and bring value to decisions? I'm grateful that I don't have to make those big decisions, but I'm grateful that I have a role in helping [our leadership] do that."

solarwinds DLT SOLUTIONS®

IT Management & Monitoring **For Government** That's Powerful, Affordable & Easy-to-Use

SolarWinds® products are designed to solve the problems IT professionals face every day. With a continuously expanding product line, that can scale to meet your needs across your enterprise, we make the most cost effective, easy-to-use IT management software available, revolutionizing the way DoD and federal IT manage their operations.

SolarWinds eliminates complexity from every IT process imaginable, including:

- Network Management
- System Management
- Security Information & Event Management
- Database Performance

Our products are easy to buy, install, use, scale, and maintain, yet still provide the power to resolve any IT management problem.

No matter what your IT challenge is, we have a product that can quickly deliver results, whether it is **network operations**, **cyber security**, **data center consolidation**, **continuous monitoring**, **scaling to the enterprise**, or **compliance**, so you can do more with less.

IT Management & Monitoring Solutions for Government

Go to
SOLARWINDS.COM/FEDERAL
to Download Fully-Functional FREE Trials

Network • Application & Server • Log & Security • Virtualization • Storage
Help Desk • File Transfer • Database Management

877.946.3751 • federalsales@solarwinds.com • solarwinds@dlt.com
SolarWinds Government

Creating a Holistic Environment with Multiple Solutions

An interview with Joel Dolisy, Chief Information Officer and Chief Technology Officer at SolarWinds

The Department of Defense is an incredibly multifaceted organization. To support that complexity, DoD personnel must craft an equally dynamic IT architecture while maintaining security. Yet considering how many separate solutions must be deployed and operated in concert, the task of creating that environment can be daunting.

However, Joel Dolisy of SolarWinds, an IT management and monitoring software provider, said that doesn't have to be the case. He explained how leveraging interoperable solutions that are dual-use and easy to operate can push the DoD mission forward.

INTEROPERABILITY REQUIRED

First, Dolisy said that IT professionals should focus on acquiring and deploying interoperable solutions. "What the military does is maintain situational awareness on the battlefield," he said. "But if you look behind the scenes at how they run their IT infrastructure, they don't have that same level of visibility."

The primary reason for this lack of transparency is that separate solutions are deployed in silos and configured without regard to how they might interact with other systems. The different acquisition schedules of DoD departments also make it near impossible to deploy a single solution across all agencies and military branches at the same time.

"DoD is extremely large and consists of many different agencies and military branches that are on different budgeting schedules," said Dolisy. "What you end up with are technologies that may not all align at the same time. You've got a kind of chicken and the egg problem."

Interoperable solutions remediate this problem. "From a level of visibility, having a unified, homogenous set of solutions across the different parts of DoD, ensuring that they share data, makes a lot of sense," said Dolisy. They can be deployed during separate budgeting cycles, yet maintain visibility across the network via their interoperability.

That's not the only benefit, either. "Just like in the private sector, as traditionally siloed departments begin to consolidate, interoperability can provide a lot of value in terms of security, adaptability, and the transfer of skills between different systems," Dolisy continued.

DUAL-USE OPTIMIZATION

To gain these additional benefits, Dolisy said that solutions should be dual-use, as well as interoperable. "What's important is that the tools being used can actually be interconnected, so that if some tools collect one type of data and that type of data can actually be useful in another tool, there shouldn't be any barrier in extracting that information to use elsewhere."

For instance, Dolisy said a tool that runs analysis on configuration management changes could create a dataset equally useful to a tool looking for network security vulnerabilities.

SolarWinds' suite of products is designed with this in mind. "Our AppStack dashboard brings together data from our server and application monitoring, virtualization manager, and storage products," said Dolisy. "We bring all of that data into a single dashboard that is easy to consume and provides powerful insights to help pinpoint where problems originate and provide remediation options. We design our products to work together."

Yet despite using a single dashboard, Dolisy explained that SolarWinds' products don't require a master system to govern all this data at once. "That would not work at the scale that DoD needs," he said. "The best thing is what's called a 'federated system,' where each entity has its own datasets and management scope, but that can roll-up within a hierarchy. So if a four-star general wants to get a picture of all the units under him, he can still do that but at a lower cost than if you actually had to collect all the data and bring it into one single command repository."

EASE OF EXPERIENCE ENSURED

More than a cost-saving measure, this ease of use is crucial to allowing IT professionals to become proficient at using the software that is already installed in the environment they manage. Dolisy explained that, as DoD's network continues to change through consolidation initiatives like the Joint Information Environment, the agency will need personnel to be able to quickly jump into tasks and become proficient at them.

"You're going to start seeing a younger IT workforce who look for intuitive software, especially as consolidation initiatives provide IT pros with more customers than before," he said. "But by implementing easy to use tools, productivity will be easier to achieve."

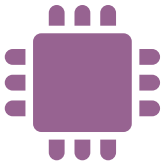
Thankfully, Dolisy sees solutions entering the market to fill these needs. "If you look at the military IT market over the past several years, it's evolved dramatically along three axes," he said. "You see software that is a lot more usable, dual-use tools that serve multiple use cases with the same data set, and interoperability as a key feature." SolarWinds focuses on ensuring all of these aspects are covered and that their solutions come together in a cohesive, deployable portfolio.


techn

Operations are changing

at DoD, and new tactics require new technologies to support them. To achieve mission success, DoD is adopting new solutions that are connected, mobile, cost-effective, and secure.

ology



ENHANCING MOBILITY

DoD employees work in every time zone and physical environment, and most of them are trying to work with people in different time zones and environments. That being the case, the **statement**, "The warfighter expects and deserves secure access to information from any device, anywhere, anytime," is unsurprising.

That's the challenge for **DoD's Mobility Program** and it's going to take a robust, multi-variant plan of action to meet expectations.

Of course, traditional mobile solutions have an important role to play in increasing connectivity between personnel and the Pentagon. Thus, DoD **has already deployed** about 1,500 unclassified phones and the Navy is hoping to deploy as many as 30,000 new mobile phones this year. Additionally, a DoD-wide bring-your-own-device pilot program is launching later this summer. **According to DoD CIO Terry Halverson**, these programs will save money, recruit talent, and improve workforce productivity.

Moreover, the department is creating programs to get the most out of these devices. For starters, DoD has an **app gallery** that provides resources in mobile-ready formats. Specific services and the department-at-large have developed solutions to cover a range of defense topics including education, training, and news.

The department has also developed more complex solutions. For example, DARPA's tablet-based **Persistent Close Air Support** program connects soldiers on the ground with aircrews, allowing them to share real-time data to enhance situational awareness and identify targets in concert. Additionally, the **Transformative Apps** (TransApps) program delivers secure data, including high-resolution map imagery, to more than 3,000 mobile devices used by troops in Afghanistan. Troops can also use the platform to update data after missions and even create new apps to meet new needs.

Yet DoD isn't stopping at smartphones and tablets. The Pentagon's mobility mission is also to grant IT capacity to warfighters abroad without first having to build an entire local infrastructure for support. To that end, it is creating mobile technologies that can operate in any environment, often at short notice.

For instance, **DARPA** is "developing a family of highly precise and accurate navigation and timing technologies that can function in GPS-denied environments and enable new cooperative and coherent effects from distributed systems." Additionally, the military is in its third iteration of setting up an ambulatory IT network to be leveraged in combat zones overseas. **This attempt**, called the Technical Control Facility in a Box, can establish a network for users to securely share e-mail messages and files.

And that's just the beginning. DoD has big plans to further enhance its technology's mobility, even going so far as to **solicit ideas** for enabling Internet communications underwater.

"The warfighter expects & deserves secure access to information from any device, anywhere, anytime."

DEFENSE INFORMATION SYSTEMS AGENCY

ACQUIRING REAL-TIME INFORMATION WITH THE INTERNET OF THINGS

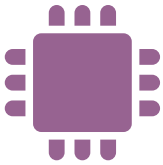
Mobility is just one piece of the puzzle when it comes to creating a truly connected defense organization. Now, even non-mobile solutions — things like tanks, airplanes, and guns — need to be connected across space and time. As **DARPA's 2015 agency report** states, "[A]dvanced hardware alone is no longer a guarantee of military and economic success; increasingly, the nation or non-state player that makes the smartest and most strategic use of that hardware will dominate." In other words, it's not just what you have but how you use it that counts.

The Internet of Things (IoT), where objects, tools, or people are used as real-time sensors, is one way the military is ensuring it gets the most out of its more static investments. By connecting sensors to existing equipment and creating new technologies that are already linked to defense networks, DoD can increase its real-time awareness of what's happening on the ground, anywhere.

This isn't necessarily a new tactic for DoD. Since 2008, the Army has **mounted sensors** in many of its troops' helmets to collect data on brain injuries suffered during combat. And if you think a little more creatively, the long-term use of radar-enabled vehicles and imaging-equipped drones puts the defense sector at the forefront of IoT.

Now, DoD is looking at ways to enhance operability. DARPA's **Near Zero Power RF and Sensor Operations** program is looking for ways to overcome the power limitations of constant data collection through sensors. JIE, mentioned earlier in this guide, will also increase the machine-to-machine interoperability of these connected devices to ensure that any system can read new data.

At the same time, DoD is expanding IoT's mission and application in defense. The increased use of drone surveillance for environmental and human terrain awareness is an obvious example of this amplified scope. Additionally, Frank Konieczny, Chief Technology Officer at the Office of Information Dominance and CIO of the Office of the Secretary of the Air Force, also **said** that DoD is considering new IoT applications for base facilities management, vehicle management, workplace security, logistics and transportation, and autonomous robotics.



EMBRACING THE CLOUD

The benefits of mobility and IoT are game-changing for the military. However, reaping those benefits (remember the big data analytics we discussed in the Operations section?) will require significant computing resources. To meet these new resource requirements, DoD is turning to cloud.

In March 2015, the Army released its **cloud computing strategy** to reach the branch's long-term objective of reducing ownership, operation, and maintenance of IT and hardware. In the foreword of that document, Army CIO Lt. Gen. Robert S. Ferrell explained that the shift "will significantly boost IT operational efficiency, increase network security, improve interoperability with mission partners, and posture the Army to adopt innovative technology more quickly at lower cost."

He isn't the only military leader who has realized cloud's advantages. Appreciating the security, cost, and operational benefits that come with moving IT functionality and systems to off-site, as-a-service computing, officials are moving all of DoD to the cloud.

The flagship of this initiative is **milCloud**, an Infrastructure-as-a-Service platform created with both commercially and government-developed technology. DISA launched it in spring 2014 across a select number of DoD data centers. This was a strong first step toward DoD in the cloud, because the as-a-service functionality offers benefits of cost reduction and flexibility.

However, the internal-only policy means responsibility for maintenance and security ultimately lies with DoD. That fact **led some industry leaders to question** if it was truly a cloud service. At the same time, many private companies were vying for opportunities to participate in DoD's cloud transformation.

Now, DoD is taking additional strides to make use of industry cloud resources. In August 2014, the Pentagon opened its networks to private cloud service providers (CSPs) by granting Amazon Web Services the first authorization to handle DoD unclassified data. Later that year, CIO Halverson released **DoD Cloud Way Forward**, a three-fold strategy to ease security requirements for CSPs maintaining certain defense datasets. DISA followed suit, **updating its cloud security requirements** to simplify the process for CSPs applying for security authorization.

DoD came late to the government cloud game, but it's making quick strides to catch up. Moving forward, many observers inside and **outside the Pentagon anticipate** that the department will continue to seek ways to better leverage industry technology and ease DISA's administrative burdens.

ENSURING SECURITY

Although these technical innovations are increasing the defense sector's efficacy and strength, they are also opening the department to new threats by creating more data and network endpoints that could be compromised. As **one department noted**, "There's evidence to show that while digital insecurity is growing, it is also making its way into devices we can't afford to doubt." Therefore, DoD is applying new security measures as it adopts these new technologies.

Within the cloud, DoD is **requesting physical separation** between classified and unclassified workloads to better segment information and prevent all-access hacks. Additionally, DARPA's **High Assurance Cyber Military Systems** (HACMS) program has worked since 2012 to secure the cyber vulnerabilities of IoT's physical systems. And for mobility initiatives, several DISA and National Security Agency pilots **are working** on ways to apply robust credentials to mobile technologies and confidently authenticate devices.

Beyond these new technology initiatives, DoD is also focusing on better securing its own networks because, as the Air Force's Konieczny **said**, "getting down to it, [we] need to secure the data. That is the crown jewel that we have — data."

The DoD cybersecurity strategy is multidimensional. It involves using internal resources to create better platforms, such as the intuitive **Plan X**, and monitor networks in real time. Other projects, such as the development of **homomorphic encryption**, are applying security to data itself.

The strategy also involves getting outside support. DARPA is soliciting ideas for new automated cyber defense systems through its **Cyber Grand Challenge** and Defense Secretary Carter **announced** that DoD is opening an office in Silicon Valley to gain better access to industry cyber tools and practice.

Finally, the Pentagon is training soldiers to become cyber warriors. In our next section, we explain how and why the workforce is changing to embrace greater security roles.

RESOURCES

ARMY CLOUD COMPUTING STRATEGY

Office of the Army Chief Information Officer, 2015

Report establishing the Army's vision for delivering cloud-enabled network capabilities across the military

BREAKTHROUGH TECHNOLOGIES FOR NATIONAL SECURITY

DARPA, 2015

Report reviewing DARPA's 2015 priorities and current initiatives to support those objectives

DOD CIO'S 10-POINT PLAN FOR IT MODERNIZATION

Former DoD CIO Teri Takai, 2012

Presentation detailing the top 10 priorities for DoD IT organizational change

DOD CLOUD WAY FORWARD

DoD, 2014

Report documenting the DoD CIO's 45-day effort to use commercial cloud services and introducing new strategies to maximize cloud capabilities

DOD CLOUD COMPUTING SECURITY REQUIREMENTS GUIDE

DISA, 2015

Guide outlining measures to securely procure and deploy cloud technologies for DoD

THE DEPARTMENT OF DEFENSE CYBER STRATEGY

DoD, 2015

Report outlining five strategic goals and implementation objectives for DoD cybersecurity

FEDERAL NETWORKS ARE BECOMING **MORE COMPLEX**

CLOUD + DATA CENTER CONSOLIDATION =

- Apps hosted farther away from federal workers
- Apps forced to travel more complex network paths

45* PERCENT — Nearly half cited **"increasing network complexity"** as the greatest federal network management challenge

27* PERCENT — One-quarter of respondents are **unable to identify** network performance challenges quickly

Over 50 percent said it takes a **DAY OR MORE (!)** to detect and fix application performance issues.

*The average cost of an enterprise application failure per hour is **$500,000 to $1 million.***

IF APPS ARE DOWN, FEDERAL WORKERS CAN'T DO THEIR JOBS

- *Lost Productivity*
- *Wasted Taxpayer Dollars*
- *Citizens Not Getting Services*
- *Low Workforce Morale*
- *Cybersecurity Risk*

Get To Know Your Apps

The Federal Network Visibility Crisis

Top Benefits of Network Visibility

- IMPROVED NETWORK **RELIABILITY** — 68%
- KNOW ABOUT PROBLEMS **BEFORE END-USERS** — 48%
- IMPROVED NETWORK **SPEED** — 41%
- MAXIMIZE EMPLOYEE **PRODUCTIVITY** — 36%
- INSIGHT INTO RISK MANAGEMENT/ **CYBER THREATS** — 35%

riverbed®

www.riverbed.com

*"Network Applications Performance PulsePoll™," Market Connections, Inc. 2015
"Realizing Business Value and ROI with Application-Aware Network Performance Management," IDC, 2012

Optimizing Mission Performance with Application Rationalization

An Interview with Sean Applegate, Director of Technology Strategy & Advanced Solutions at Riverbed Technology, Federal

Over the years, organizations often acquire numerous applications with the objective of improving operational efficiency. However, when those same applications become obsolete or duplicative, they are not always removed, optimized, or even accounted for. This can reduce efficiency and force organizations to waste resources on technology with little to no operational value.

The Department of Defense is no exception to this issue, but there is a solution. Application rationalization can address this challenge and improve efficiency. To learn more about application rationalization, especially as it relates to DoD, we spoke with Sean Applegate of Riverbed Technology, a leader in application performance infrastructure.

IDENTIFYING & CONSOLIDATING APPLICATIONS

Application rationalization is the process of identifying applications across multiple services, finding duplication, and consolidating them to a smaller number of enterprise applications. The process also moves these modernized applications to a more secure, centrally located datacenter.

"If you look at something like a core datacenter, or MilCloud, or FedRAMP-certified cloud, those are common places this new application will be hosted," said Applegate. "In the long term, this will bring down operational costs and allow continuous improvement."

The strategy goes beyond just improving efficiency of applications, however. "At a high level, benefits of application rationalization really focus on [applications being] better aligned with the mission itself," Applegate said.

RATIONALIZING EFFECTIVELY

To successfully rationalize applications, Riverbed uses a six-step process:

1. Discover and map out your applications portfolio. It's important to understand what your applications dependencies are and how they're currently performing. "We do that very well here at Riverbed, from high level usage, all the way down to the individual transaction level," said Applegate.
2. Assess the performance of the application and the environment, to determine the business alignment of each application. This can be scoped out using solutions from Riverbed, Applegate noted.
3. Rationalize the application. Examine the performance of current technology and understand potential changes. "By using prediction technologies, we can understand how performance and connectivity will be impacted if an application is moved, prior to actually moving it," Applegate said. This facilitates strategic planning and impact analysis.
4. Migrate the application. Unexpected barriers may occur, so it is important to monitor the environment during the migration process so problems can be resolved promptly. "At Riverbed, we can provide acceleration solutions that allow us to migrate the data faster from one datacenter to a future datacenter or cloud," said Applegate.
5. Operate in production. Examine the impact, and determine the degree to which efficiency and effectiveness of processes have been improved.
6. Continuously improve. It is important to understand your environment as it changes, recognizing strengths and room for improvement. What can be optimized? What facilitates a controlled, high-quality experience?

UNDERSTANDING BENEFITS & BARRIERS

"Application rationalization allows us to integrate multiple applications together more easily," said Applegate. "But it also means moving away from a siloed approach." This integration ties applications to the mission of the organization and facilitates an effective end-to-end experience for the user.

However, there are some common barriers to application rationalization. And this is not to be taken lightly, as the cost of application failures can range from $500,000 to $1 million per hour per failure, according to Applegate.

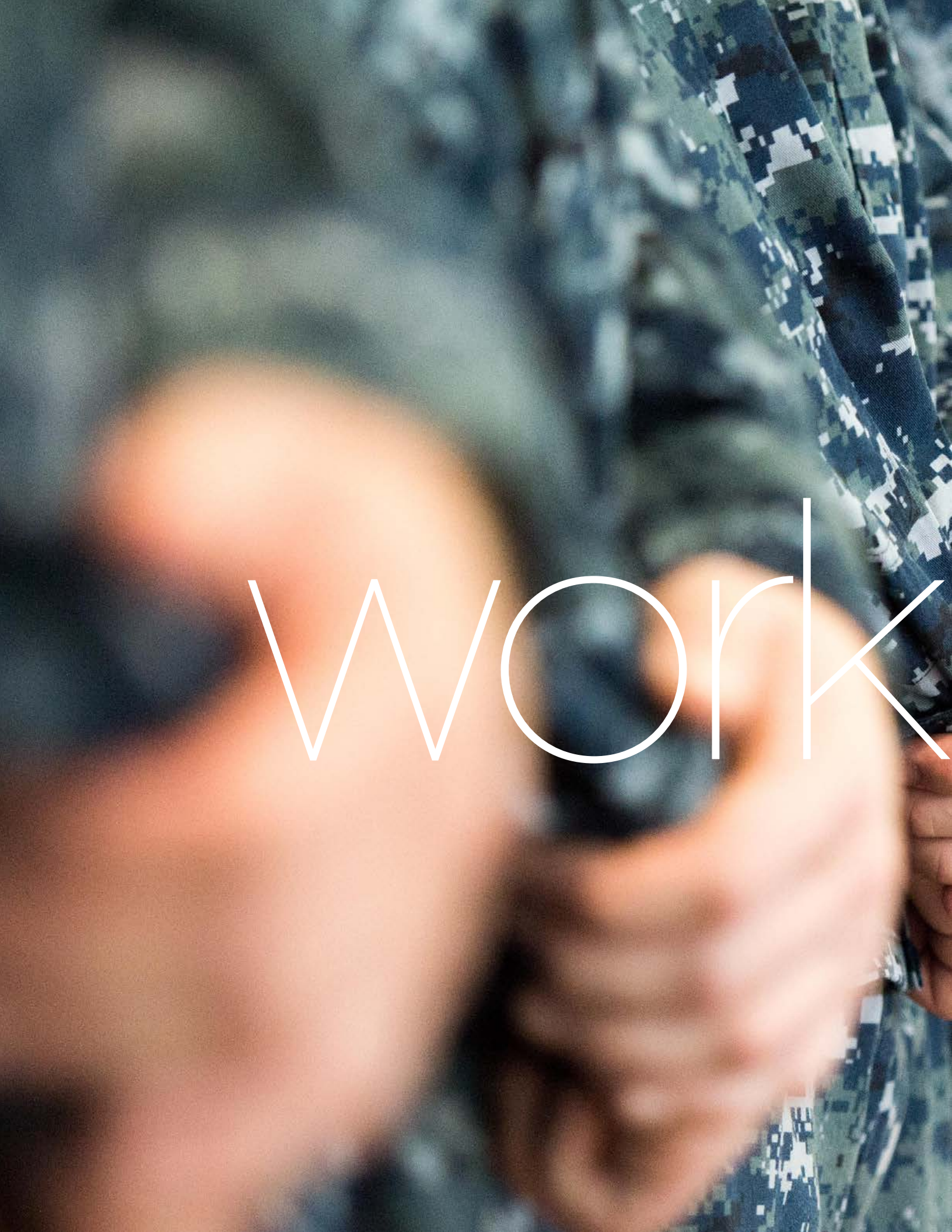
For one, agencies may not view their applications from an end-to-end system approach, failing to consider the multitude of stakeholders across the DoD landscape. "If different user scenarios aren't designed into the application construct very effectively, end-to-end performance suffers, and thus the mission itself suffers," said Applegate.

Disruption during the migration phase is also common. "There's typically a lot of dependencies that can cause performance issues and create fragility in the application," said Applegate. "It's ideally identified before the migration, but often when you do the migration, other things might be identified that you just weren't aware of."

However, when these barriers are overcome, there are significant benefits. Applegate explained how Riverbed freed up about 20 percent of an organization's computing power and reduced its costs significantly. Core applications were running smoothly on average, but Riverbed found that one older application was consuming a disproportionate amount of resources, slowing down the rest.

"When we fixed that application by replacing it with a newer modern piece, we eliminated the need for about 2,000 CPUs," said Applegate. "That was a huge cost savings that was hidden in the averages. That's where detailed application performance management solutions can expose things you don't normally see."

In DoD, that can be the difference between a warfighter accessing an operational brief in three to five seconds instead of minutes. "Those are very real savings for the mission," said Applegate. By speeding up and optimizing applications, mission velocity is improved. And mission performance is what really matters in the long run.


work

As new threats emerge,

a revamped defense workforce must be recruited and trained to keep ahead of the adversary. The Pentagon is addressing these concerns by improving its service member readiness, realigning resources toward vulnerabilities, and adapting its personnel management strategy.

force

IMPROVING READINESS WITH VIRTUAL TRAINING

When you think about the armed forces, training drills and strenuous obstacle courses may be the first things to come to mind. These traditional exercises are crucial to basic training, but remaining a cutting-edge force requires new, innovative methods.

In fact, some experts already observed **the return of "tiered readiness,"** meaning only those stationed in conflict zones or those next in line for deployment are trained to peak readiness. What's more, only 23 percent of DoD employees surveyed in a Government Business Council **report** said they believe that current training levels will meet the military's readiness needs. To remedy this skill gap without a wartime budget, DoD has turned to live, virtual, and constructive (LVC) training to improve readiness.

According to DoD's 2010 **Strategic Plan for the Next Generation of Training**, effective training in the new era of defense must account for:

- Full spectrum operations in any battle space
- The ability to use technologies and techniques that support geographically unconstrained training
- The ability to maintain competency against a traditional enemy while actively fighting a complex, elusive, and adaptive adversary

LVC training — virtual training with computer-based simulations that can be integrated with live training — can help meet these requirements. In fact, the same DoD strategic plan states that LVC capabilities are an integral component of building a balanced and versatile joint capable force.

Each military service has begun developing significant virtual simulation capabilities. For example, the Army's flagship training game, Virtual Battlespace 3 (VBS3), is a three-dimensional, first-person military training simulation program. Facilitated by U.S. Army Training and Doctrine Command's (TRADOC) **Combined Arms Center-Training**, VBS3 provides an immersive and realistic gaming environment with flexible scenario and terrain options. VBS3 has been accredited to support more than 102 combined arms training tasks, such as breaching an obstacle, establishing an observation post, and conducting an artillery raid. **To test VBS3** early in the development process, TRADOC's Army Capabilities Integration Center used **Early Synthetic Prototyping** (ESP), which uses a virtual environment to allow soldiers to assess and give feedback on emerging training programs.

At the Department of the Navy (DON), the Office of Naval Research (ONR) Augmented Immersive Team Trainer program is developing a system for Marine observer training that users wear on their heads. The system incorporates simulated objects and effects, such as explosions or enemy vehicles, with real terrain.

This simulated environment is known as "augmented reality," which **overlays sensory input** such as sound, video, or graphics on a view of the real world. The idea is to more fully immerse users in the simulation and enhance their understanding of the environment.

"If you shoot a mortar round and miss, you can determine how much you missed and then adjust," **said** ONR Manager for Human Performance Training and Education Peter Squire. "It allows you to train with those kinds of capabilities," while avoiding the expense and safety risk of using real weapons.

Increasing simulated/synthetic training resulted in an estimated annual savings of **$119 million** for the Navy and about **$1.7 billion** for the Air Force between fiscal years 2012 and 2016.

However, dollars saved lose their significance if training quality suffers. **Many DoD officials worry about fidelity**, or the extent to which virtual training matches reality. But virtual training has actually been shown to outperform live training in skills and knowledge transfer to trainees. **A 2011 review of studies** concluded that, "Computer-based simulations…show positive results [and] in 22 out of 26 such studies, trainees demonstrated equal or superior transfer to the control group from simulations."

There will always be a need for live training; some situations and exercises just cannot be replicated adequately in simulations. But as a supplement to other training to improve performance levels and combat skill decay, LVC training is enhancing the way the military readies warfighters.

PIVOTING TO CONFRONT CYBER CHALLENGES

Despite the increasing pervasiveness of cyberthreats, there is no government-wide strategy to build a highly trained federal cybersecurity workforce. This is especially concerning considering the United States' cyber workforce shortage.

DoD is ahead of the curve in solving the problem. It created a **Cyberspace Workforce Strategy** in December 2013, which outlined six focus areas for the organization:

1. Establish a cohesive set of DoD-wide cyberspace workforce management issuances.
2. Employ a multi-dimensional approach to recruiting.
3. Institutionalize continuous learning with greater focus on evaluating the maturity of skills.
4. Retain qualified personnel.
5. Expand threat knowledge.
6. Understand crisis and surge requirements and options.

To implement the strategy's first focus area, the department is drafting a Cyberspace Workforce Framework. In this effort, DoD is leveraging the National Initiative for Cybersecurity Education Workforce **Framework** to provide structure and content to define skill requirements.

With high-level strategy taking shape, the Pentagon has also taken definitive action on the ground through the creation of U.S. Cyber Reserves. DoD has already experimented with reserve units that specialize in the cybersecurity mission. The Department will train these "**surge forces**," who will help defend the energy sector, telecommunications and other critical infrastructure, **said** Defense Principal Cyber Adviser Eric Rosenbach in a Senate Armed Forces subcommittee hearing. When there is a conflict or disaster, reservists will be **quickly mobilized**.

Rosenbach noted that nearly 2,000 Reserve and National Guard personnel will also support the Cyber Mission Force, part of the department's Cyber Command (CyberCom).

Planned to be operational by fiscal 2018, the Cyber Mission Force will include 133 teams made up of about 6,200 soldiers and DoD civilians. According to CyberCom's **written statement**, the force will defend military networks, defend the United States against attacks of "significant consequence" and conduct "full-spectrum operations" for "contingency plans and military operations."

Similarly, the **Defense Cyber Crimes Center** provides basic and intermediate computer forensics training for **all DoD components**, plus some agencies outside the department.

In light of these advances, Defense Secretary Carter **said** he sees the cyber workforce as a trailblazer for how the department can welcome new ideas and embrace a younger generation of professionals. CIO Halvorsen had similar thoughts, **noting** that the model for developing the cyber workforce could be used in the future for other budding fields across DoD.

But with the present cyber talent gap and CyberCom only **half-staffed**, DoD has much work left to do in developing the cyber workforce before it considers implementing this model elsewhere. Along these lines, the next section focuses on DoD's efforts to recruit and retain top talent.

MEETING THE NEEDS OF TODAY'S SERVICE MEMBER

Developing a cyber workforce plan is a smart strategic move, but the Pentagon intends to improve its overall workforce tactics — especially retention — across all service branches. **Some see** the **Defense Officer Personnel Management Act** (DOPMA) as forcing the armed forces into a system that awards seniority over ability and constrains the flexibility to recognize and fast track the highest performers to positions of greater responsibility.

Those who want reform **argue that** the management system created in the 1940s to serve a draft military is not meeting the demands of the 21st-century, all-volunteer force. After all, DOPMA itself is more than 30 years old but many of its provisions are based on its much older predecessor, the Officer Personnel Act of 1947. Ultimately, this chases some of the most talented officers out of the service, which can have serious consequences.

Because legislative reform is outside the scope of DoD's power, leaders are addressing the issue in other ways. For example, Carter recently **laid out** his "**Force of the Future**" vision for reforming the military's manpower policies.

First, he plans to expand "sabbatical programs" that allow personnel to take time off from active duty without harming their careers. The Navy was the first to test the program in 2009, followed by the Marine Corps in 2013, and the Air Force and Army last summer. Sabbatical programs provide service members the option to spend up to three years outside active duty while retaining health benefits and remaining competitive for future promotions.

Similarly, Vice Admiral William Moran, Chief of Naval Personnel, proposed a system of **"on ramps" and "off ramps"** that would allow sailors to transition between active duty and the reserves throughout their careers. Further institutionalization of the sabbatical program and statements of support from leadership will help boost the use of this option, which currently remains low.

The **second strategy** is to create a path for individuals to enter the military in the middle of their careers at relevant mid-level ranks. A vast majority of service members must begin their careers at entry-level ranks, but individuals with certain specialized skills, such as doctors, lawyers, or cybersecurity professionals, could benefit from this approach. For example, it would be much easier to entice an industry computer engineer into the service starting as a major, as opposed to a second lieutenant.

On the other hand, the Army is looking to help those who started their careers in the service. The Army Reserve's Cyber Private-Public Partnership, or **Cyber P3**, will help service members with cyber skills obtain employment at major companies such as Lockheed Martin, Citibank, and Microsoft.

Finally, Secretary Carter **proposed** a college loan repayment option for service members with specialized skills. With the rising cost of higher education, this is a strong incentive. Additionally, the Office of Personnel Management granted DoD special hiring powers for cybersecurity recruits. This will allow the Pentagon to bypass the traditional competitive criteria, fast tracking the hiring of civilian professionals who have unique cyber skills and knowledge. The **pay scale** for the new defense positions starts at about $42,400 and goes up to just more than $132,000.

Reforming the current workforce system is critical, but DoD faces obstacles. These new methods — especially the loan repayment option — are appealing but costly given that the Pentagon is already struggling with personnel costs. Another major hindrance is the department's lack of control over many of its own personnel policies. For example, sabbatical programs and similar policies **cannot be legally created** without congressional authorization. Furthermore, DoD is having difficulty accounting for general personnel requirements, according to a GAO **report**. This makes it difficult to **identify efficiencies** and make the business case for additional requirements.

Despite these challenges, the Pentagon is making strides toward establishing hiring practices that are more amenable to the talent its components require.

RESOURCES

CYBER IN-SECURITY II: CLOSING THE FEDERAL TALENT GAP

Partnership for Public Service & Booz Allen Hamilton, 2015

Research report examining cyber workforce issues and providing recommendations for improvement

DEPARTMENT OF DEFENSE CYBERSPACE WORKFORCE STRATEGY

DoD, 2013

Directive outlining the six key strategic areas that will drive and transform DoD's cyber workforce

DEPARTMENT OF DEFENSE STRATEGIC PLAN FOR THE NEXT GENERATION OF TRAINING

DoD, 2010

Strategy identifying areas of improvement and providing recommendations to ensure DoD sustains operational and training superiority

GOING VIRTUAL TO PREPARE FOR A NEW ERA OF DEFENSE

Government Business Council, 2015

Research report examining the workforce readiness challenge and how virtual training can help

NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

National Initiative for Cybersecurity Education, 2012

Guidelines providing a common understanding and lexicon for cybersecurity work and roles in order to develop and retain a top-quality workforce

SECURING GOVERNMENT: LESSONS FROM THE CYBER FRONTLINES

GovLoop, 2015

Research guide examining five cyber tactics to keep government secure, including DoD insight on the Cyberspace Workforce Strategy

THE VIRTUAL TRAINING PLAYBOOK FOR GOVERNMENT

GovLoop, 2015

Research guide examining how to enhance the efficacy of virtual training, including through DoD case studies

The future of technology is more secure than ever.

Intel® Security combines the expertise of McAfee® with the performance and trust of Intel to deliver secure computing to consumers and businesses worldwide. We believe that as technology becomes more deeply integrated into life, security must be more deeply integrated into technology. Because when everyone has the confidence to use technology to its full potential they can achieve their full potential. Visit www.intelsecurity.com.

intel® Security

McAfee is now part of Intel Security.

Beyond Security: How Endpoint Protection Facilitates Mission Success

An interview with Scott Montgomery, Vice President and Chief Technology Strategist at Intel Security

In an increasingly interconnected world, securing every network endpoint is a major challenge, especially for an organization as large as DoD. More connections, while improving communication, collaboration, and efficiency, also mean more vulnerability and a larger attack surface.

To explore the issue further, we sat down with Scott Montgomery of Intel Security. He discussed the challenges DoD faces in the evolving field of endpoint security, why DoD-accredited solutions are key, and how Intel Security's solutions achieve security and optimize operations for mission success.

OVERCOMING COMMON ENDPOINT CHALLENGES

According to Montgomery, when it comes to next generation endpoint security, finding the right technology is not necessarily the challenge. Instead, the slow pace of acquisitions and accreditation are major barriers to adequate capabilities. As a result, the DoD is working with the same technology they bought years ago. That's a problem. "If you think about the pace of change in technology, there's nothing from 2006 still in use today by anybody for anything," said Montgomery.

The complex and evolving nature of endpoints makes aging tech even more problematic. "What constitutes an endpoint has changed pretty dramatically since DoD did their first contract for Host Based Security System (HBSS) in 2007," Montgomery said. "Is a wearable an endpoint? Is a mobile phone an endpoint?"

If a device includes mission data, Montgomery argues it certainly constitutes an endpoint worth securing. Even a thermostat can be considered an endpoint. With so many connected devices, knowing how much of the IP landscape they can cover with just one system is going to be one of the biggest challenges DoD faces, said Montgomery.

UNDERSTANDING DoD NEEDS

Intel Security is addressing these challenges by building solutions made specifically for DoD. "We built a vast array of technology that's managed by the same single console that DoD is familiar with," said Montgomery. "The cost to transition to the next generation of this technology, if they choose this option, is actually far lower than anything else. And for endpoints, we include those things that make the DoD different."

That means serving specific DoD communities and their respective data needs with modular solutions. For example, a garrison at a fort would not need the intense amount of bandwidth that a tactical brigade using satellite communications would need.

"A lot of vendors don't build for that crucible of the tactical community," said Montgomery. "And we absolutely are ready to be there."

Importantly, this past experience with DoD makes Intel Security solutions cost-effective. DoD can reuse existing infrastructure because Intel Security utilizes the same console for the technologies DoD is consuming today. On the other hand, the cost to roll out a wholly new solution would be "staggering," said Montgomery.

"DoD can leverage what they already have. What they need to do is change the contract in order to encompass these new pieces of technology," he said. "We're the lightest fit-out of anyone from the cost standpoint, even considering the next generation endpoint opportunity, because we're already there. We built a very modular system that can encompass a variety of different technologies in the same offering."

Another benefit of this association is DoD accreditation. "Many vendors have built commercial offerings that have never been accredited in DoD," said Montgomery. "Accreditation is a staggeringly expensive and difficult thing to do."

THINKING BEYOND SECURITY

Once endpoint security solutions are deployed, vendors need to think outside the box. When every offering is a security offering, what other benefits are included? Montgomery cited freeing up resources and less "chair-swiveling" as some key benefits.

During missions, warfighters' main focus should be on running the mission package. "If your information security and privacy system reduces the amount of overall effort on operations, you're going to be more effective against the adversary," said Montgomery. "In the tactical community, information security should be the last thing warfighters have to worry about. What they should be focused on is mission assurance."

The solution should also reduce what Montgomery called "chair-swiveling." Having multiple agents on multiple consoles is very time consuming. "They have to look multiple places in order to make a determination of what's going on, make an assessment of whether it's dangerous, and then act," said Montgomery. "If we aggregated those functions in one console, the whole operation would be more effective. The unit would be more efficient because more of their time would be spent on analysis and mission assurance than on chair-swiveling."

In the critical world of defense, every second counts. This is why next generation endpoint security solutions need to offer more than security alone. Improving operational efficiency for the warfighter could be the difference between mission failure and mission success.

From Sailor to Cyber Warrior

An interview with retired Navy Captain Mark Hagerott, PhD, Deputy Director and Distinguished Professor of Cyber Security, U.S. Naval Academy

The threats facing our defense systems and networks are daunting. To successfully address these challenges, we need talented military personnel to lead the charge. The U.S. Naval Academy, fresh off of its **2015 Cyber Defense Exercise victory**, is helping make that happen. To learn more, we spoke with Mark Hagerott, PhD of the U.S. Naval Academy. He explained what they're doing in Annapolis to prepare our nation's next generation of exceptional cyber professionals.

SHARING KNOWLEDGE & EXPERIENCE

The Navy had a head start in the game of cyber and electronic warfare. "The British controlled the undersea cables, so the U.S. Navy moved to wireless systems, and has been dealing with wireless electromagnetic jamming, and then eavesdropping for 115 years," Hagerott explained. "Now the rest of the world is doing it."

Learning early lessons from electromagnetic cyber warfare, the Navy recognizes that cyber has implications across all parts of its branch. That's why it has established the Center for Cyber Studies within the Naval Academy.

As deputy director of the center, Hagerott wants to improve knowledge sharing and interdisciplinary research. Wherever possible, he seeks collaboration with research entities, especially with the Office of Naval Research on important information dominance and cybersecurity initiatives. "The center's mission is to enhance the education of midshipmen in all areas of cyber warfare," said Hagerott. "And then integrate this knowledge across the faculty to avoid stovepiping."

FOCUSING ON CYBER

The Naval Academy also recently formed a Cyber Science Department that offers a cyber operations major for a modest number of midshipmen. The first cohort to graduate with this degree will do so in 2016.

"We have all these midshipmen that are coming through, and we need to get them exposed to cyber," said Hagerott. "That's the other function of the program, which is why we have two, brigade-wide mandatory courses which shape the education of 4,000 future officers."

The program goes far beyond exposure, however. The rigorous curriculum requires an exceptional level of interdisciplinary skills that test mental, intellectual, and physical limits.

"We give them a foundation in the basics, for example, what binary is, what hexadecimal is, how a computer functions. Students will actually take a computer apart, so they can see where the memory is and where the hard drive is. The idea is to give them a sense that this isn't mystery or magic — it's actually a machine they can control," said Hagerott.

In addition to physical computer architecture, midshipmen will gain competencies in the complex subject areas of programming, data structures, networks, database systems, information assurance, cryptography, and forensics. Due to its difficulty, the program is not for everyone.

"Certain people have an affinity for coding and understanding the artificial world of computers and networks. I remind them that the machine is not natural, and they should not get discouraged if they struggle to understand the machine with the aim to keep control of it," Hagerott said. "[Nonetheless], you have to have an ability to sit at a keyboard and communicate and interact with a computer, and write and create languages, or create programs using languages."

Hagerott explained that some midshipmen are unable to meet these requirements and have had to drop out of the program. He provided a useful analogy: "You just don't create classical pianists," he said. "There are some people who can really relate to octaves and keyboards, and other people who cannot. Brains are mapped in different ways."

CREATING WELL-ROUNDED CYBER PROFESSIONALS

On top of the computational and technical skills, cyber majors must also balance their program with courses in areas such as policy, law, ethics, and social engineering. As an emerging field, cyber operations is not just about computer science or information technology.

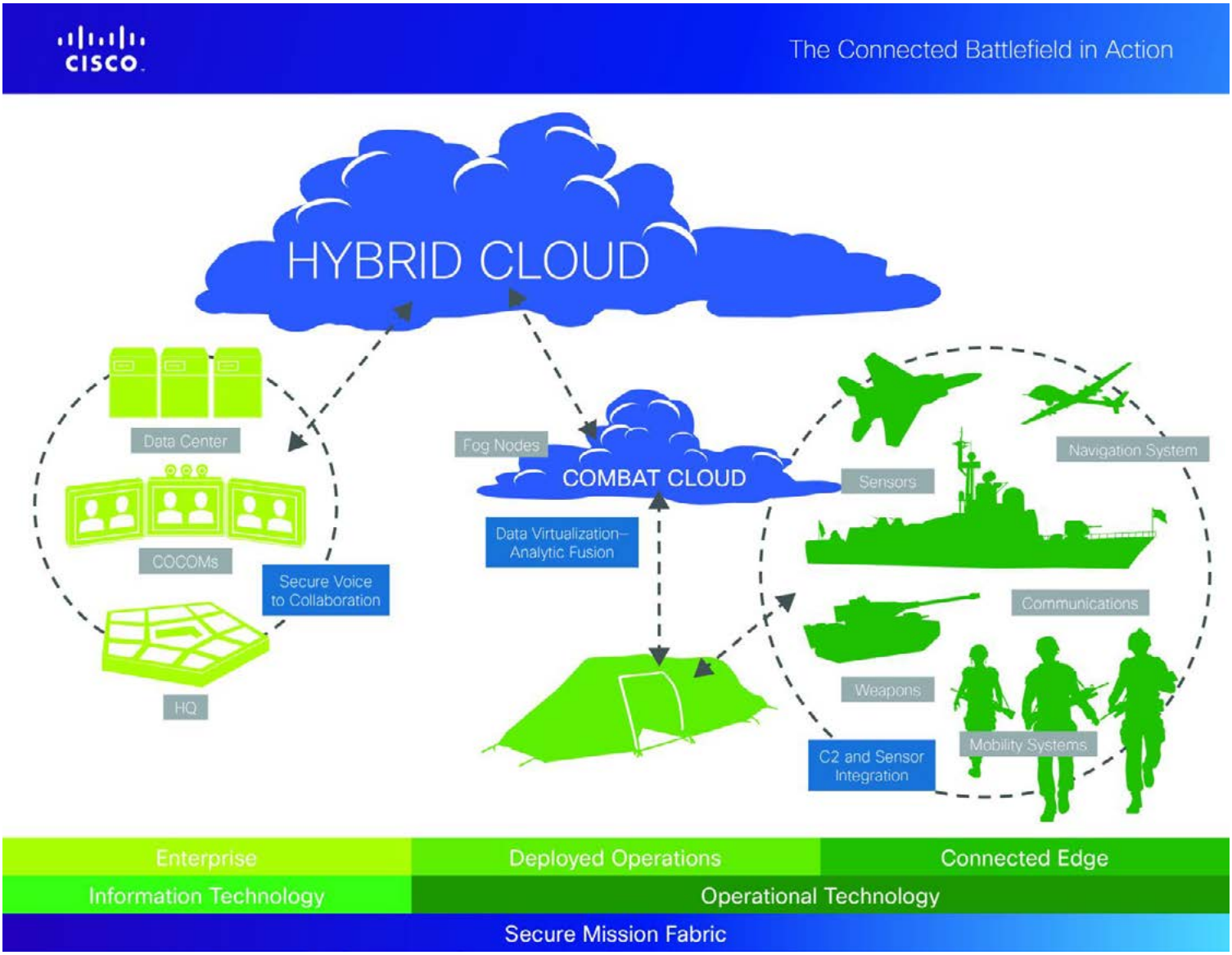
"Cyber is becoming an integration of human and machine, made possible through a mutually understandable language. But for those officers who will be responsible to control and protect the human-machine world of cyber, they need to take some social science courses and write and research policy. You can't just have coding skills alone," said Hagerott.

He also noted the importance of trust and integrity. Following the Edward Snowden case, for example, some courses now focus on such things as criminal psychology and insider threats.

On top of the technical and non-technical skills, graduates must also be physically fit in order to perform their traditional naval duties, such as standing 18-hour watches, climbing through submarine hatches, or operating in hot engine rooms.

"You can see how these necessary requirements create a smaller and smaller pool," said Hagerott. "You have to be able to program in Python, C, understand machines as well as social elements, and then, by the way, be able to sustain yourself and your body in rigorous physical environments."

This ensures that those who make it through the program are really the best of the best. This is important because, when faced with a formidable challenge, preparation must be equally rigorous. By developing exceptional cyber professionals with broad and diverse skillsets, the U.S. Naval Academy is enhancing the capabilities of our nation's defenses to counter and advance against cyber adversaries.



The Internet of Everything (IoE)

IoE is delivering on the DoD vision of network-centric warfare; to translate information advantage through IT into competitive advantage on the battlefield.

Why Cisco?

The future is here. From next-generation networks to industry-leading mobility, cloud, and video, Cisco provides the secure, integrated architectures that connect people, process, data, and things. The network is the universal enabler for global communications, collaboration, data sharing, and analytics. It is the platform that connects organizations, people, and machines, and it enhances mission effectiveness by improving efficiency and decision making in modern and effective ways. Together with Cisco, the DoD can achieve the vision of network-centric warfare by creating an secure mission fabric that connects the enterprise to the edge.

For more information, visit www.cisco.com/go/defense

Achieving Real-Time Defense with the Internet of Everything

An interview with Nick Michaelides, Senior Director of Federal - Defense, and Gary Hall, Chief Technology Officer of Federal - Defense, at Cisco

The mission of DoD, "to provide the military forces needed to deter war and to protect the security of our country," remains steadfast. Yet the barriers to accomplishing that mission are increasing.

Nick Michaelides of Cisco summed up those difficulties. "Defense leaders are dealing with lots of challenges both internally and externally, and they're operating in an environment of constant and accelerating change," he said. "Technology innovation is speeding up, business needs are evolving, and the geopolitical landscape is shifting. What's more, the traditional conflict between nations has recently been replaced by more asymmetrical warfare and cyberthreats."

So how does DoD combat these changing threats? Michaelides, along with his CTO Gary Hall, explained how the Internet of Everything (IoE) could provide real-time, situational awareness of defense systems when it's supported by digitization and effectively secured.

LEVERAGING THE INTERNET OF EVERYTHING

IoE, put simply, is the connection of sensors to devices, places, and even people to generate real-time data and situational awareness. This idea holds great potential for the defense sector.

"IoE brings together people, processes, data, and things to provide better information for military decision-making," said Michaelides. "The Internet of Everything has the potential to deliver on the DoD vision of network-centric warfare, to translate information advantage through IT into competitive advantage on the battlefield."

Not only does IoE generate crucial data to inform operations, but it also has the potential to increase DoD's response time. "IoE extends the reach of IP connectivity out to the tactical edge," Michaelides said. "It goes well beyond the old connectivity, to what we now refer to as fog computing, which enables real-time analytics and allows for a very rapid response to the changing conditions you find on the battlefield."

DIGITIZING THE DOD NETWORK

However, to take full advantage of these sensors requires the department to upgrade its networks and digitize operations. "The Internet of Everything is about connecting devices, data, people, and processes," explained Hall. "Digitization is what happens when collaboration, data, and processes are brought onto a digital medium. They're really very closely interrelated. IoE creates value through connections and digitization builds on that value through analytics, efficiency, automation, and process improvement. The Internet of Everything is driving digitization across all types of organizations."

As it leverages more sensors, DoD is no exception to the trend of digitization. "Digitization of defense will allow our military to take advantage of the exponential value of connected devices and services to transform operations, meet the needs of the workforce and citizens, and provide what we believe to be a superior capability on the battlefield," said Michaelides.

ENGRAINING CYBERSECURITY

However, as DoD's networks are linked to real-time sensors through digitization, there is an obvious concern: cybersecurity. Michaelides acknowledged that new connections bring new vulnerabilities, but he also asserted how a proactive stance can mitigate those risks. "We need to stay ahead of the threats while taking advantage of these [IoE] connections," he said. "DoD will have to deploy more agile and flexible IT infrastructures and services that are purpose-built for cybersecurity."

Hall agreed: "You have to protect at the endpoint, and at the application level from the endpoint through the transport medium, into your IT network."

In order to achieve this end-to-end security, DoD will have to determine and deploy cybersecurity requirements before new sensors are installed. "A total threat defense can't be tacked on after resources are deployed or moved to the cloud," he said. "To effectively protect against cyberattacks, the military must take more of an architectural approach that protects at multiple layers and avoids gaps in protection."

Of course, building this holistic IT architecture is a complex task. Hall explained how his team can help. "Cisco is a strategic partner," he said. "We can help deliver the architectures and services that enable DoD to take advantage of the value of all of these emerging disruptive technologies."

By integrating security into every deployed component, DoD can confidently reap the benefits of a digital environment, informed by IoE.


acquis

If there is one component

of DoD that will ultimately hinder or enable the pursuit of its goals, it is acquisitions. This is the strategy by which every piece of DoD is defined and procured in order to empower, train, and equip today's warfighters. To keep pace with evolving needs and technologies, DoD will infuse its acquisitions strategy with greater flexibility, better-trained professionals, and industry partners.

sitions

ATTAINING BETTER BUYING POWER

The driving force behind DoD's acquisition strategy is an initiative called **Better Buying Power** (BBP), originally launched in 2010 to help the department "do more without more." Although the department continues to confront challenges of a post-9/11 world, its budget is unlikely to reach its 2001-02 pace in the near future. Recognizing that incongruous reality, BBP is dedicated to realizing **seven core focus areas:**

- Achieve Affordable Programs
- Control Costs Throughout the Product Lifecycle
- Incentivize Productivity and Innovation in Industry and Government
- Eliminate Unproductive Processes and Bureaucracy
- Promote Effective Competition
- Improve Tradecraft in Acquisition of Services
- Improve the Professionalism of the Total Acquisition Workforce

After five years, DoD is already citing successes across many of these objectives. One example is the Navy's acquisition of three DDG 51 Class Guided Missile Destroyers. After traditional sole-sourcing negotiations stalled (a common problem in acquisition), the Navy used BBP tactics to shorten the acquisition timeline, use multiple contract types, and ultimately increase competition among industry applicants. As a result, the destroyers were acquired in an unprecedented amount of time: It took less than six months from decision to compete to contract award. Additionally, the Navy cited $298 million in savings as a result of the reduced timeline and competitive pricing.

One reason BBP has reaped such rewards is its openness to change based on lessons learned. The initiative's primary purpose is to enhance DoD acquisition by enabling agile processes. Therefore, it makes sense that it is developed with agility, undergoing constant improvement and redesign to focus on the defense sector's changing needs.

Currently, BBP is in its **third iteration**, themed "Achieving dominant capabilities through technical excellence and innovation." Although Version 2.0 focused on enhancing efficiency and productivity in spending, the latest initiative is dedicated to ensuring DoD maintains technological superiority through innovation on any battlefield, including cyberspace.

EMPOWERING ACQUISITION PROFESSIONALS

As exemplified in the Naval destroyer example, part of BBP's approach is to offer alternative, more flexible contracting vehicles that enable swifter procurement.
But these agile procedures are only one piece of the acquisition puzzle. For DoD to truly find value in new procedures, the department must also have professionals who can strategically use them. Thus, DoD is exploring a variety of avenues beyond procurement procedures in order to better empower acquisition professionals.

The goal of BBP 3.0 is **to remove** many of the side jobs and external burdens professionals face so they can focus solely on acquisition. At the same time, the initiative wants to increase DoD support for science, technology, engineering, and math (STEM) education so that personnel have sufficient understanding of the projects and designs they procure. To that end, BBP 3.0 will also require higher qualifications for acquisition specialists and program leaders of research and development projects.

To ensure resources are available to support these training initiatives, DoD is working with Congress. In 2008, Congress vested $4.5 billion in the newly established Defense Acquisition Workforce Development Fund to increase recruitment and training of acquisition professionals. This year, the House Armed Services Committee is proposing the **Agile Acquisition to Retain Technological Edge Act** to extend and formalize that program, under guidance from DoD officials. The act would enable "proactive, agile, transparent, and innovative" acquisition, not only by funding recruitment and training, but also by providing robust career paths for military officers interested in acquisition.

Finally, military services are working to integrate acquisition across silos to give professionals the resources and intel they need to make appropriate decisions regarding requirements and procurement vehicles.

One example of this tactic comes from the Army. Learning from **recent attempts** to procure "mobile protected firepower" — essentially, a tank that can be easily transported and airdropped — General H.R. McMaster says the new rule of Army acquisition is, "Do it together and collaborate from the beginning." Now, relevant stakeholders including operations staff, acquisitions professionals, and Army Materiel Command will all work together to determine requirements. Additionally, the branch will no longer separate the requirements stage from the greater acquisition process to ensure that details and goals aren't lost in the handoff stage.

"Do it together and collaborate from the beginning."

GENERAL H.R. McMASTER
US ARMY

COLLABORATING WITH INDUSTRY

In addition to integrating acquisition with other agency partners, DoD is also working toward better collaboration with industry. Besides providing technology, industry partners can offer lessons learned from their own R&D processes and they often have a better understanding of what capabilities can be harnessed at what cost. Bringing these knowledge resources into the DoD acquisition chain, however, requires better collaboration between defense and commercial sectors.

The Navy's Innovation Cell is **one mechanism being used** to drive that collaboration. In its first round, the program seeks industry solutions to military needs, with a particular focus on big data analytics, virtualized desktops, and network architecture for unified communications. But rather than seeking technology alone, officials want to work with industry leaders to decrease the transition time from commercial IT to the Navy IT environment. By soliciting feedback and working collaboratively across the acquisition lifecycle, DON will learn best practices for running pilots, communicate and formulate requirements with development partners, and discover what acquisition procedures and procurement laws should be altered to speed innovation.

The **Air Force is also taking a partnership approach** to acquisition through its own new program, Bending the Cost Curve. It was designed through a months-long series of roundtables between Air Force officials and industry leaders, in which they discussed ways to help each other achieve common acquisition goals. The resultant initiative is multifaceted, with two components already underway.

One aspect is the smaller Cost Capability Analysis (CCA) program, which will leverage industry perspectives to set more realistic requirements and lower pricing of effective weapons systems. Four programs, the T-X jet trainer, the Long-Range Standoff Weapon, the Multi-Adaptive Podded System, and the Space-Based Infrared System follow-on, were chosen as pilots for CCA because they are each in a different place in the acquisition cycle and represent different military use cases.

Additionally, the Air Force is expanding the extant PlugFest program, an annual DoD forum in which vendors showcase their new solutions, to include a direct contracting capability. The new PlugFest Plus will combine a low-barrier, Army acquisition model with the industry event to allow the Air Force to contract with exhibitors within just a few weeks. That way, Air Force acquisition professionals are empowered to make real-time decisions with industry partners at the showcase

RESOURCES

AGILE ACQUISITION TO RETAIN TECHNOLOGICAL EDGE ACT

Rep. Mac Thornberry (R-Texas) of the House Armed Services Committee, 2015

Bill proposing the extension of 2008 pilots, and implementing new reforms, to make the DoD acquisition system "proactive, agile, transparent, and innovative"

BETTER BUYING POWER 3.0 IMPLEMENTATION GUIDANCE AND FACT SHEET

DoD Acquisition, Technology and Logistics, 2015

Resources outlining priorities and implementation of third version of DoD's acquisition plan

ACQUIPEDIA

Defense Acquisition University, 2015

Online portal provides definitions and resources for defense acquisition professionals

DOD WEAPON SYSTEMS ACQUISITION: 2015 HIGH RISK REPORT

U.S. Government Accountability Office, 2015

Report summarizing the current state and high risk pitfalls of the current defense acquisition system

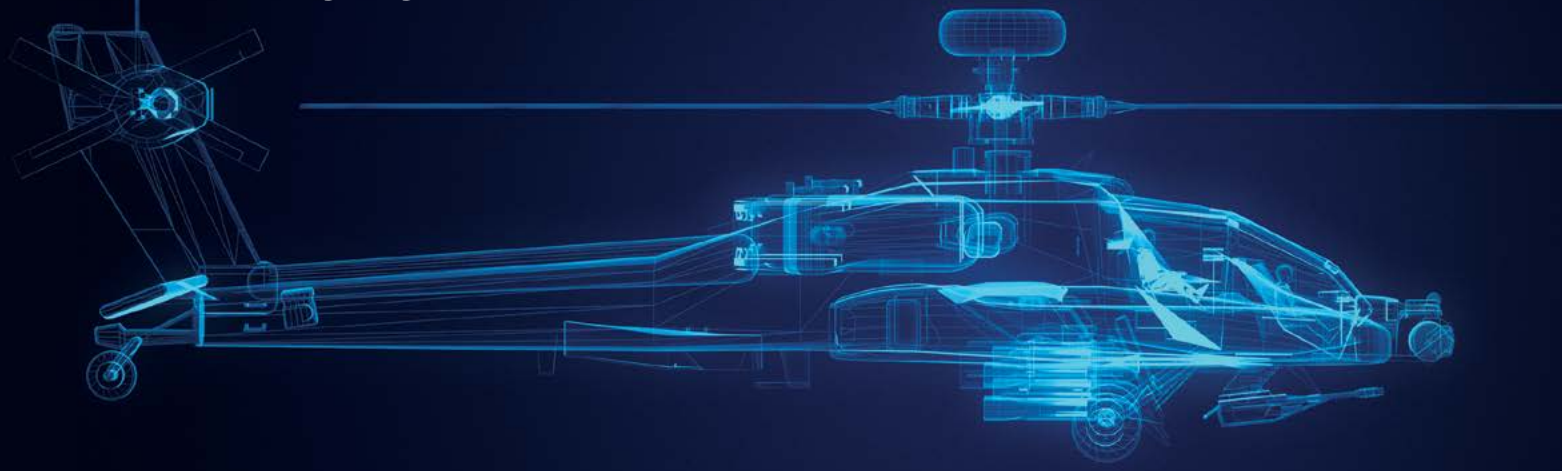
DEFENSE AT&L

Defense Acquisition University

Bi-monthly magazine covering the latest defense acquisition news and providing commentary on common acquisition challenges

Defense National Security Solutions

Transforming digital experiences for mission success.



Adobe is the global leader in digital content solutions. The U.S. Department of Defense leverages Adobe tools and services to create ground-breaking digital content, deploy it across media and devices, measure and optimize it over time, and achieve greater mission success. Defense solutions from Adobe are a Joint Information Environment (JIE) standard* to make, manage, mobilize, secure, and measure mission-critical digital content. U.S. defense agencies achieve greater mission success and efficiency with Adobe.

The Adobe Advantage

DEFENSE NATIONAL SECURITY PROGRAMS

Defense Imagery & Video Processing	Cybersecurity & Continuous Monitoring	Training & Simulation	Public Affairs & Engagement
Digital Recruiting & Human Resources	Mobile Applications & Mission Planning	Contracts & Procurement	Digital Publications

www.adobe.com/government

/AdobeGov @AdobeGov

* Not all standards apply to all Adobe products.

Using Smart Content to Make Sense of Data in the DoD

An interview with Craig Bowman, Vice President of Defense and National Security at Adobe

The Department of Defense is unique in many ways – but one commonality it shares with many other organizations is the issue of trying to make sense of its data.

DoD is rising to the challenge. To understand how the department is using "smart content" to make sense of their data and help people find the information they are looking for, GovLoop spoke with Craig Bowman at Adobe.

CONFRONTING BIG, UNSTRUCTURED DATA

"Growing data and trying to make sense of the data has been a challenge for the Defense Department and the intelligence community for a long time," Bowman explained. "This is compounded by the fact that the data itself is changing. Most of our data now is very unstructured. That's the videos, images, audio files, and documents that we're now collecting – and these files are critically important for our workforce and for our mission."

But the number of these files presents DoD with a challenge. "The problem with those kinds of data files is, while you may be able to find them in research, actually getting the meaning out of them is difficult," Bowman said. "We call that challenge deep data – as opposed to big data."

Bowman said big data is the vast collection of files and data. In contrast, deep data is understanding how you find the small part of the file or data that's relevant to what you're actually looking for. "An analyst can find the video of the IED of interest, but if the video is 12 hours long, it may take them all day to find piece that is relevant," he said.

That's where Adobe's approach helps DoD with this challenge.

LEVERAGING SMART CONTENT

Bowman explained smart content as such: "If you look at the commercial sector, the way that this is being used is very easily understood," he said. "If you are using a smartphone and you are walking by a Best Buy, suddenly you get an advertisement, and the advertisement says, now on sale at Best Buy, 50% off blank CDs. You don't actually have to search for a sale to be notified of one. We call those kinds of interactions, engagements."

But quickly creating those kinds of on-the-fly relationships at an organization like DoD can be difficult in a solely relational database environment, especially involving aspects like images, videos, geolocations, and different security settings.

But with Adobe's smart content approach, the content can be made to be in a state to be matched against its perfect pair of a person that needs it. "Adobe's engineers are hard at work finding new ways to match similar video segments, audio patterns, and images," said Bowman. "While the push to innovate in these areas are mostly driven by commercial needs, we plan on using them to support our DOD mission."

"The parameters of the object help define who should get it, and the moment the person enters the sphere of influence of that content, systems can match up content to the individuals and deliver to them in near real time," Bowman said. "And so that's what we talk about when we say smart content. The content is marked, and is therefore smart enough to know that, for example, I'm restricted to top-secret users, or I'm restricted to a certain geolocation. So it builds its own pedigree, if you will, of who would be interested in looking at the content and who's allowed to look at it and where are they allowed to look at it."

PROVIDING BATTLEFIELD SUPPORT

An example of how this could revolutionize DoD? Bowman said to look to the warfighter in the field.

"If data becomes smartly aligned to people based on who and where they are, then everybody becomes a data attractor," Bowman said. "Let's take a soldier. When a soldier is holding his weapon, he can't really use a device in his pocket that he has to pull out and hit the button with his thumb. But what if you mount it on their inside forearm? They can look at it while they're holding their weapon."

Continued Bowman, "But then the question became, well how are they going to do a search; how are they going to look for the things that they need to find without taking their finger off the trigger? And we said, let's take the same advertising paradigm and deliver something other than an ad. We already know who they are, where they are, and what they're doing. And we'll be able to deliver them personalized intelligence in real time without them ever touching the device."

Added Bowman, "This innovation is critical. When it comes to trying to change the way we do things in the future, we have so many restrictions in the government, and so many rules. Our enemies don't. Our enemies are able to capitalize on all of the technology available to them, while we are often still stuck in procurement. But agile innovations that embrace smart content will help us change the future of DoD."

An OASIS for Army Contracting

An interview with Harry Hallock, Deputy Assistant Secretary of the Army (Procurement)

As the General Service Administration's (GSA) largest customer with nearly $3.5 billion in contracts, the Army needs to do procurement right. That's why its recent sign-on with One Acquisition Solution for Integrated Services (OASIS) is a big deal. To learn more about this agreement and why it's so important, we spoke with the person who committed the Army to use OASIS, Harry P. Hallock, Deputy Assistant of the Army (DASA) for Procurement.

In March, Hallock signed a memorandum of understanding (MoU) with GSA, guaranteeing the Army will spend at least $500 million annually through OASIS – a target Hallock feels the Army will easily hit.

According to the GSA, OASIS is a multiple award, government-wide acquisition vehicle that provides flexible and innovative solutions for complex professional services. These core services cover the following disciplines: program management, management consulting, logistics, engineering, science, and finance. Hallock says OASIS will enable strategic sourcing, promote flexibility, expand partnerships, and ultimately improve the way Army does procurement.

ENABLING STRATEGIC SOURCING

Noting the goal of continuous acquisitions improvement, Hallock is excited about the potential of OASIS. "Leaders are always looking at how we're buying services and how we can do it better," Hallock said. "I think DoD and the civilian agencies have all been trying to get better and smarter at buying services and, along with that, strategic sourcing."

Strategic sourcing, continuously improving and revaluating purchasing activities, allows agencies to be more efficient on a limited budget. "This is an opportunity to…look at an instrument that meets our needs and basically frees up our limited contracting resources, enabling us to concentrate on our core mission – the writing, execution, and oversight of contracts," said Hallock.

The contracting mission, in turn, supports soldiers in the field and also procures weapons systems. More ancillary-type services, such as post or station support, are still important but don't necessarily need to be done via Army procurement vehicles.

PROMOTING FLEXIBILITY

With the GSA running the initial procurement instrument, the Army can improve management and contract oversight. Local contracting organizations will still complete the actual task order against OASIS, but the contracting instrument is not located on-site – it's with GSA.

"The benefit is that people will start realizing you don't need to have that contract instrument written by your local contracting

organization in order to get the service you're asking for," Hallock said. "So, to me that's going to be a big deal in the Army."

Furthermore, using the OASIS contracting vehicle is not mandatory, but has instead been introduced as a new strategic initiative for consideration. "When contracting officers are looking at how they're going to meet a specific contracting requirement, I want them to look at [OASIS] as one of the options and then justify whatever option they pick, whether it's OASIS or some other instrument," Hallock said.

BRANCHING OUT

As a contracting vehicle, OASIS allows the Army to engage new companies. "I look at OASIS as an opportunity for us to expand our horizons," said Hallock. "When repeatedly working with the same companies, we tend to forget that if we spread our net wider, we could potentially get new business on board."

However, this change isn't embraced by everyone, especially those in industry who did not make the business decision to go after the OASIS contract. But Hallock explained that those companies could potentially partner with other companies that are already on the OASIS contract, or there's the possibility that GSA may allow those companies to modify their stance on OASIS.

MAKING A COLLECTIVE DECISION

OASIS offers many procurement benefits, but the MoU decision was not taken lightly. Despite the Air Force signing up with OASIS about a year ago, Hallock explained why the Army didn't sign up right away.

"I wanted to make sure that we looked at the pros and cons and I wanted to make sure I canvassed the field for input; that took a little bit of time," he said. "But frankly, I don't have a problem with us taking the time when we're looking at making a good business decision."

Furthermore, taking time to discuss the decision with stakeholders led to confidence and buy-in. "People like to be heard and even if the decision isn't the one they wanted, the fact that they got their say in the decision is always a good thing," Hallock said.

This involvement and communication can also prevent rumors and negativity. Hallock explained that leaders are sometimes hesitant to communicate if there is uncertainty, but this should not stop them.

"Even to say, 'Hey, we haven't figured this out yet,' – that's communication," said Hallock. "And that's better than no conversation or giving the naysayers the chance to develop a 'worst case' scenario."

DOING PROCUREMENT BETTER

Moving forward, Hallock's ultimate vision is for the Army to use OASIS to buy the vast majority of the previously mentioned services.

"When you look at OASIS, this is one of the first very big contract opportunities and instruments to do strategic sourcing across the entire federal government," he said. "I'm excited about the possibilities here and the opportunities to look across the entire federal government to see how we can improve our business practices as stewards of taxpayer dollars."

Acquia THINK AHEAD.

Acquia is the digital experience company.

We provide software, solutions and services that empower government agencies to build, deliver and optimize websites on our open digital experience platform. Acquia helps agencies foster greater digital engagement with citizens and securely deliver information and services with greater efficiency, agility and resiliency.

OPTIMIZE
Convert audiences with contextual content across every device and channel
Acquia Lift

DELIVER
Launch and manage sites quickly on the resilient cloud DevOps love
Acquia Cloud

BUILD
Bring content, social and commerce experiences together
Drupal

STATE OF GEORGIA →

CITY OF LOS ANGELES →

AFT →

AUSTRALIAN GOVERNMENT →

HHS →

To learn more about how we help our customers succeed visit acquia.com/government.

Updating the Department of Defense with Open Source

An interview with Dan Katz, Public Sector Technical Director at Acquia

When you think of DoD's information infrastructure, you might think mostly of complex, secret networks. Yet the reality is that the department maintains thousands of public-facing websites to inform civilians and personnel alike. What's more, keeping those portals functioning and up-to-date can be as challenging of a task as any other defense operation.

To understand how DoD might achieve this task, we spoke with Dan Katz of Acquia, an open source digital platform solutions and services provider. He explained how embracing an open content management system (CMS) and digital cloud platform offers DoD the agility to securely respond to changing needs and environments, as well as gaining efficiencies and saving taxpayer dollars.

SIMPLIFYING WEBSITE MANAGEMENT

The most obvious benefit of an advanced CMS is its ability to streamline website management. "An open cloud platform allows DoD to consolidate multiple sites and standardize on a proven robust technology stack," said Katz. "For example, the Navy has thousands of websites, on a variety of different technology stacks, and they're actively looking for easy, cost effective models for managing and deploying those."

One of the difficulties in managing those multiple websites is the breadth of their complexity. Katz said a fleet commander website could be as simple as six pages while other sites could comprise hundreds of pages. "They're spending a tremendous amount of tax dollars on software licenses as well as on the resources to manage these," he said.

Using services such as Acquia Cloud Site Factory allows organizations to manage multiple websites with less difficulty. "Standardizing on an open digital cloud platform would allow the Navy and any DoD organization to centrally manage sites based on common templates," Katz said. "It would allow them to centrally procure cloud platform services, and it would also allow non-IT users and content managers who are moving around to different posts to not be dependent on IT when a new site needs to be spun up."

MAINTAINING AGILITY

This usability by non-IT personnel is the key to the cloud platform's second benefit, agility. "The biggest benefit of choosing an open platform is you have tremendous innovation and agility advantages, so that you can quickly adapt to changing conditions," said Katz. "No organization as much as DoD needs to be able to do that."

Content managers are able to update content as soon as conditions or environments change, ensuring they meet the most pressing information needs. At the same time, "Those freed-up IT staff can be focused on innovating and providing mission critical solutions for the warfighters," said Katz.

SECURING PUBLIC & PRIVATE NETWORKS

While these content and operational benefits are necessary for DoD to remain relevant, some officials may be hesitant to adopt an open solution due to security concerns. However, Katz said these concerns are unfounded.

He explained that using open cloud platforms does not require exposing your entire network. "If I were DoD, I wouldn't want every site visitor traversing my network to see public information. One of the primary benefits of a cloud platform would be to keep the public outside of my network," he said.

Moreover, department leaders are already putting safeguards in place to ensure that open platforms can be used to their fullest potential without sacrificing security.

"The new DoD CIO, Terry Halvorsen, is now accepting FedRAMP, which is the civilian government standard for cloud security, for DoD levels 1 and 2. That's the equivalent to a FISMA moderate accreditation," explained Katz. "Public facing websites with non-sensitive data can live on those cloud platforms and be completely segmented from internal networks in DoD. If there is a need to have some integration to other systems in DoD, cloud platforms like Acquia can use VPN and VPC technologies to have a secure end-to-end isolated network connection between the public cloud and DoD networks like NIPRnet and the Defense Research Engineering Network."

PARTNERING FOR SUCCESS

What's more, service providers like Acquia can help ease the transition and maximize outcomes. "An organization can't just go ahead and download Drupal and start implementing this at an enterprise level," said Katz. "You really need to be conscious about choosing a partner that has experience with the technology and knows how to implement it in an enterprise environment like DoD."

This partnership is imperative not only from a security perspective but also from an organizational change perspective. "It's not just a technology issue," Katz said. "There are governance issues and people issues that are often times the most complicated and challenging. Only a vendor that has that experience is going to be able to help DoD be successful."

Open source cloud platforms are the way forward for DoD. However, the department doesn't have to undergo this transition alone.

The DoD of Tomorrow

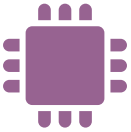
This guide describes a wide variety of new programs, strategies, and investments within the U.S. defense sector. But many of these are just getting off the ground. Today, DoD is in a fluid state of change. Assuming it overcomes the challenges of misperceptions, change aversion, and bureaucratic malaise, the DoD of the future will truly be a force to be reckoned with. Here, we offer a brief timeline of how the agency was organized yesterday, how it's changing today, and what government leaders hope DoD will look like tomorrow.

YESTERDAY

OPERATIONS

- Operated without technology or data standards resulting in numerous systems that were not interoperable
- Leveraged top-down, Waterfall project management techniques
- Made decisions based on anticipated outcomes

TECHNOLOGY



- Relied on local software, IT infrastructure, and custom platforms
- Leveraged IoT in basic forms
- Maintained local security systems with traditional tactics

WORKFORCE

- Offered limited variety of training options
- Required basic combat readiness
- Managed personnel in an inflexible system that diminished top talent retention

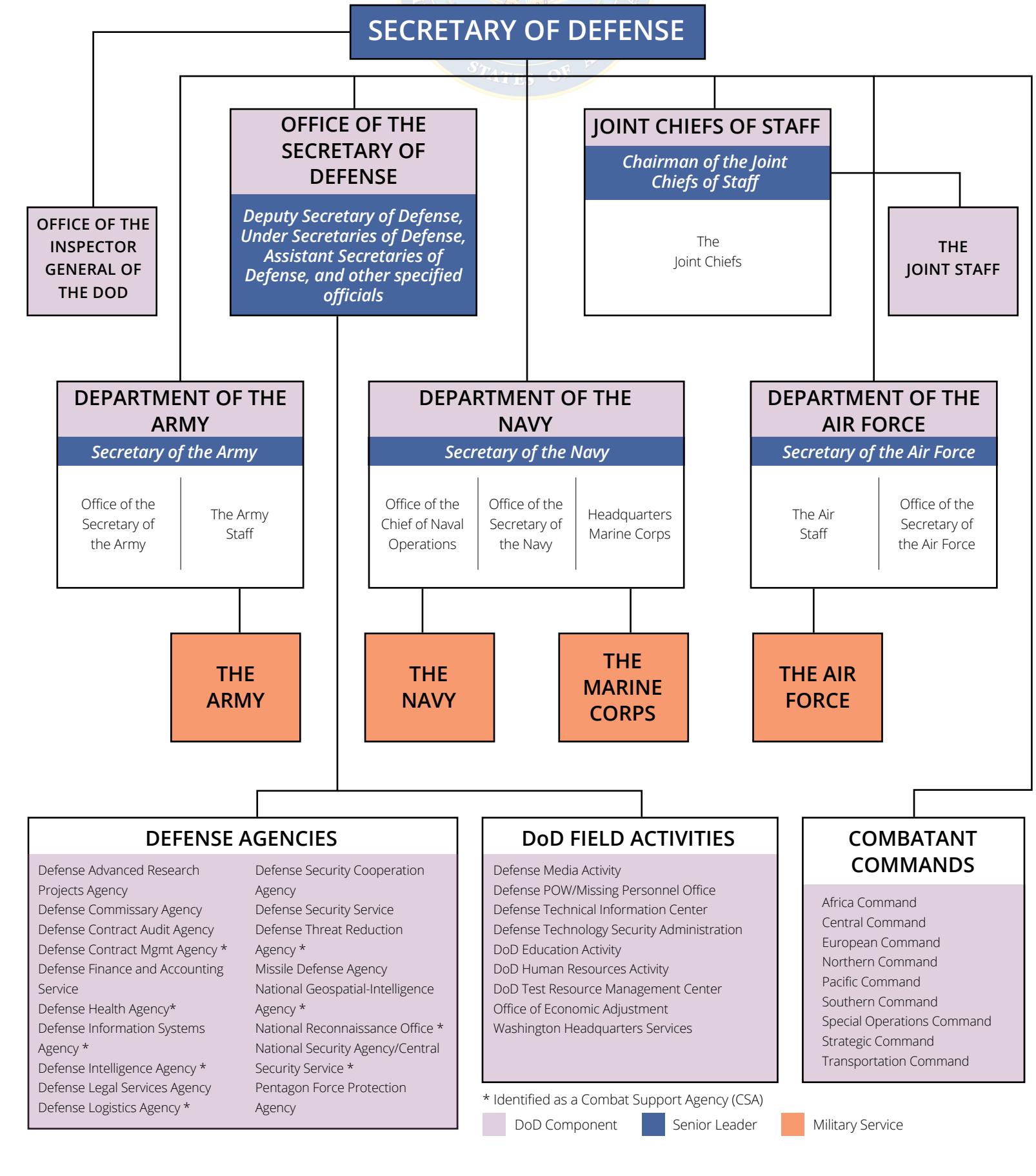
ACQUISITION

- Unable to keep pace with industry because of cumbersome procurement vehicles and procedures
- Taxed acquisition professionals without providing appropriate training
- Minimized contact with commercial sector, outside of formal procurement

TODAY	TOMORROW
⁘ Consolidating and standardizing operations ⁘ Enabling Agile project management ⁘ Powering decisions with data	⁘ Interoperable across platforms and missions ⁘ Flexible and adaptive to meet new mission needs ⁘ Capable of making informed decisions based on real results
⁘ Embracing the cloud ⁘ Enhancing mobility ⁘ Acquiring real-time information ⁘ Ensuring security	⁘ Connected across environments, missions, and teams ⁘ Powered by enhanced, pay-per-use, off-site services ⁘ Monitored for cyber insecurity across technologies and networks
⁘ Improving troop readiness with virtual training ⁘ Pivoting to confront cyber challenges ⁘ Meeting the needs of today's service member	⁘ Trained across a wide variety of simulated and live options as basic requirement ⁘ Fully staffed cyber workforce with specific roles identified and delineated ⁘ Improved and institutionalized initiatives, such as sabbatical programs, leveraged to enhance career flexibility
⁘ Attaining better buying power ⁘ Empowering acquisition professionals ⁘ Collaborating with industry	⁘ Equipped via adaptable, efficient procurement models ⁘ Staffed with a cadre of highly-trained acquisition teams ⁘ Apace with innovations in the private sector, due to robust partnerships with industry

ORGANIZATION OF THE

DEPARTMENT OF DEFENSE



ACKNOWLEDGMENTS

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 150,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to **info@govloop.com.**

1101 15th St NW, Suite 900
Washington, DC 20005
Phone: (202) 407-7421
Fax: (202) 407-7501
www.govloop.com
@GovLoop

THANK YOU

to Acquia, Adobe, Cisco, DLT Solutions, Intel Security, Riverbed Technology Federal, SolarWinds, and Tanium for their support of this valuable resource for public sector professionals.

AUTHORS:

Hannah Moss, Researcher and Writer
Matthew Garlipp, Research Fellow

DESIGNERS:

Jeff Ribeira, Creative Manager
Tommy Bowen, Graphic Designer
Kaitlyn Baker, Design Fellow
Daniella Conti, Design Fellow

PHOTO CREDIT:

Department of Defense, Joint Chiefs of Staff, US Army, US Marines, US Navy

1101 15th St NW, Suite 900, Washington, DC 20005
Phone: (202) 407-7421 | Fax: (202) 407-7501
www.govloop.com
@GovLoop